



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002372910 A**(43) Date of publication of application: **26.12.02**

(51) Int. Cl.

**G09C 1/00****G06F 12/14****H04N 5/91****H04N 5/93**(21) Application number: **2001182956**(71) Applicant: **VICTOR CO OF JAPAN LTD**(22) Date of filing: **18.06.01**(72) Inventor: **SUGAWARA TAKAYUKI  
SHICHJO SHUNICHI**

(54) **AUTHENTICATING AND REPRODUCING  
METHOD FOR CONTENTS INFORMATION AND  
CONTENTS INFORMATION AUTHENTICATING  
AND REPRODUCING DEVICE**

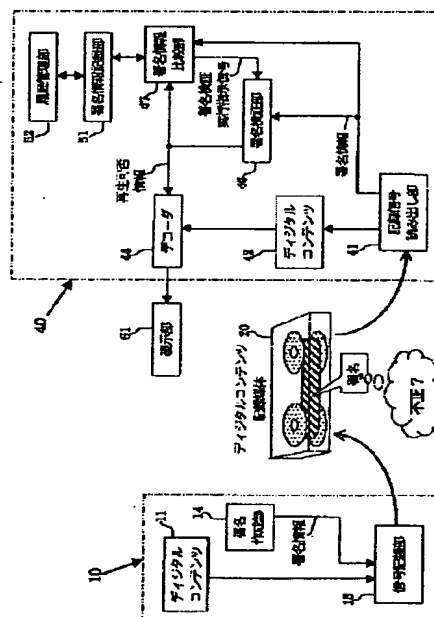
as the unauthorized signature information and the reproduction of the contents is stopped.

COPYRIGHT: (C)2003,JPO

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a contents reproducing device extracting contents to which unauthorized signature information is attached by verifying a signature and denying its reproduction and reproducing only digital contents to which right signature information is attached by a simple signature verification.

**SOLUTION:** By collating signature information recorded on a recording medium together with the digital contents with the unauthorized signature information to be an unauthorized object stored in a storage medium beforehand, when matching information is present, the reproduction of the contents is denied or stopped without performing the processing of authentication. Also, when the matching unauthorized signature information is not present, the signature information is verified. When it is verified as the unauthorized signature information, the unauthorized content information is additionally stored in the storage medium







## 【特許請求の範囲】

【請求項1】 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とを記録したデジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報の認証再生方法であって、

前記デジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る第1のステップと、

正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する第2のステップと、

その第2のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第3のステップと、

前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第4のステップと、

を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【請求項2】 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とが伝送されるデジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報の認証再生方法であって、

前記デジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る第1のステップと、

正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する第2のステップと、

その第2のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第3のステップと、

前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第4のステップと、

を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【請求項3】 正当な権利の基に制作されたデジタルコ

ンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とを記録したデジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報認証再生装置であって、

前記デジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る記録信号読み出し手段と、

正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段と、

その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段と、

前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段と、

を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【請求項4】 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とが伝送されるデジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報認証再生装置であって、

前記デジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る情報信号受信手段と、

正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段と、

その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段と、

前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段と、

を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【請求項5】 前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、取

り外し可能な可搬型記憶媒体である前記署名情報記録手段に記憶された前記不正署名情報群を用いて行うことを特徴とする請求項3又は4記載のコンテンツ情報認証再生装置。

【請求項6】前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、ネットワークに接続されるネットワークサーバの記憶媒体に記憶される前記不正署名情報群のデータを得、その得られたデータを用いて行うことを特徴とする請求項3又は4記載のコンテンツ情報認証再生装置。

【請求項7】前記署名検証手段における署名検証は、前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段を有するネットワークサーバに、前記再生署名情報をネットワークを介して伝送すると共に、前記ネットワークサーバより前記署名検証の結果に係る情報を得て行うことを特徴とする請求項3又は4記載のコンテンツ情報認証再生装置。

【請求項8】前記署名検証手段における前記デジタルコンテンツの再生中止に係る動作は、そのデジタルコンテンツ情報の復号を行う復号器に、再生が不許可であることを示す再生不可情報を供給して復号を中止する動作であることを特徴とする請求項3又は4記載のコンテンツ情報認証再生装置。

【請求項9】前記署名検証手段における前記デジタルコンテンツの再生中止に係る動作は、前記デジタルコンテンツに付されるコピー許可情報がコピー許可であるとされる場合であっても、そのコピーのためのデジタルコンテンツ信号の他の記録媒体への供給を中止する動作であることを特徴とする請求項3又は4記載のコンテンツ情報認証再生装置。

【請求項10】前記署名情報記録手段における前記再生署名情報の前記不正署名情報群への追加は、可搬型である記憶媒体に追加記憶するようになすことを特徴とする請求項3又は4記載のコンテンツ情報認証再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルコンテンツ及びそのデジタルコンテンツを記録した記録媒体の認証再生方法に関するもので、特に不正な署名情報の検証方法、及びそのデジタルコンテンツが再生されたときの処理方法、更にその方法を搭載した装置に関する。

【0002】

【従来の技術】従来より、著作権で保護されるデジタルコンテンツが、不正にコピーされた記録媒体の利用を防止するための有効な手段として、署名による認証を行う方法が一般的になされている。その認証再生方法は、記録媒体に、デジタルコンテンツの他に、その記録媒体あるいはコンテンツが正当なものであることを示す署

名情報を記録し、その署名情報を基にコンテンツ再生の許可、不許可を与えるようにしてコンテンツの再生制御を行うものである。

【0003】そのデジタルコンテンツの再生制御が行われる装置では、まずその署名が正当なものであるかどうかを検証され、正当なものであるとされるときにのみデジタルコンテンツの再生が行なわれるようにしている。

【0004】そして、特開2000-22680号公報「デジタルコンテンツ流通方法及びコンテンツを再生可能に記録した記録媒体」には、署名の検証結果を基に、少なくとも一部を暗号化したデジタルコンテンツの復号化に必要な鍵を復号化するかどうかを判断し、署名等の情報が有効であると判断されたときにコンテンツを復号する方法が開示されており、そのような署名によりコンテンツ再生の制御を行う方法は知られている。

【0005】

【発明が解決しようとする課題】しかしながら、上記の方法で用いられるような署名を用いる方式では、署名情報の改竄等に対する保護に一定以上のセキュリティレベルを確保しようとするときに、署名及びその署名の保護に係る必要なデータ量は大きくなり、かつ署名の認証に用いられる演算量も多くなり、その認証処理は複雑になる。

【0006】そして、その署名の認証を行うためには十分な処理能力のあるパソコンを用いて行う等の信号処理のための作業環境が必要であるが、一般のユーザが利用可能なデジタルコンテンツ再生装置にはそのような処理能力の高いコンピュータシステムを搭載することは再生装置の価格が高価になり好ましくなく、通常は署名認証のための処理能力が低くされる場合が多い。

【0007】そのような処理能力の低い署名認証機能しか有しないデジタルコンテンツ再生装置では、ユーザによる再生操作がなされた後にコンテンツが再生されて表示されるまでには多くの時間が必要とされ、しかもそのような複雑な署名認証処理をコンテンツの再生毎に行わなければならない、そのようなデジタルコンテンツ再生装置は再生動作が開始されてからコンテンツが表示されるまでに時間を要してしまうなど、使い勝手の良い機能を実現するために障害となるなどの課題があった。

【0008】そこで、本発明は、コンテンツ及びそのコンテンツを記録した記録媒体が、正当なコンテンツ及び記録媒体であることを示す署名情報を記録した記録媒体から情報を再生するに際し、コンテンツ及び記録媒体の認証を行い、不正なコンテンツ及び媒体であると認められたときはコンテンツの再生を不許可もしくは停止するようなデジタルコンテンツ再生方法において、記録媒体に記録される認証情報を、予め記憶媒体に記憶される不正対象となる署名情報と照合し、一致する情報が存在するときは前記認証の処理を行わずに、コンテンツの再

生を不許可もしくは停止するようにした。

【0009】また、一致する情報が存在しないときは、その新しいコンテンツ及び記録媒体の署名に係る認証作業を行い、不正なコンテンツ及び媒体であると認証された場合には、その不正対象となる署名情報を、取り外し可能なメディア、ないしはメモリ素子に記憶する、又はその署名情報をネットワークインターフェースを介してネットワークに接続されるサーバシステムの記憶装置に記憶するようにして、予め記憶媒体に記憶される不正対象となる署名情報の更新を行なうようにし、コンテンツ再生の際に行われる署名情報の認証作業が簡略化されたコンテンツ情報の認証再生方法、及びその方法を搭載するコンテンツ情報認証再生装置の構成を提供しようとするものである。

【0010】

【課題を解決するための手段】本発明は、上記課題を解決するために以下の１）～１０）の手段より成るものである。すなわち、

【0011】１） 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とを記録したデジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報の認証再生方法であって、前記デジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る第１のステップ（４１）と、正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する第２のステップ（４７）と、その第２のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第３のステップ（４６）と、前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第４のステップ（５１）と、を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【0012】２） 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とが伝送されるデジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報の認証再生方法であって、前記デジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る第１のステップ（４９）と、正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちの

いずれかと一致するか否かを検出する第２のステップ

（４７）と、その第２のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第３のステップ（４６）と、前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第４のステップ（５１）と、を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【0013】３） 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とを記録したデジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報認証再生装置であって、前記デジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る記録信号読み出し手段（４１）と、正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段（４７）と、その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段（４６）と、前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段（５１）と、を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【0014】４） 正当な権利の基に制作されたデジタルコンテンツと、そのデジタルコンテンツの制作者の認証に係る署名情報とが伝送されるデジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報認証再生装置であって、前記デジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る情報信号受信手段（４９）と、正当な権利の基でなく制作されたデジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段（４７）と、その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記デジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出

されないときは前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段(46)と、前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段(51)と、を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【0015】5) 前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、取り外し可能な可搬型記憶媒体である前記署名情報記録手段に記憶された前記不正署名情報群を用いて行うことを特徴とする3)又は4)項記載のコンテンツ情報認証再生装置。

【0016】6) 前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、ネットワークに接続されるネットワークサーバの記憶媒体に記憶される前記不正署名情報群のデータを得、その得られたデータを用いて行うことを特徴とする3)又は4)項記載のコンテンツ情報認証再生装置。

【0017】7) 前記署名検証手段における署名検証は、前記再生署名情報が前記デジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段を有するネットワークサーバに、前記再生署名情報をネットワークを介して伝送すると共に、前記ネットワークサーバより前記署名検証の結果に係る情報を得て行うことを特徴とする3)又は4)項記載のコンテンツ情報認証再生装置。

【0018】8) 前記署名検証手段における前記デジタルコンテンツの再生中止に係る動作は、そのデジタルコンテンツ情報の復号を行う復号器に、再生が許可であることを示す再生不可情報を供給して復号を中止する動作であることを特徴とする3)又は4)項記載のコンテンツ情報認証再生装置。

【0019】9) 前記署名検証手段における前記デジタルコンテンツの再生中止に係る動作は、前記デジタルコンテンツに付されるコピー許可情報がコピー許可であるとされる場合であっても、そのコピーのためのデジタルコンテンツ信号の他の記録媒体への供給を中止する動作であることを特徴とする3)又は4)項記載のコンテンツ情報認証再生装置。

【0020】10) 前記署名情報記録手段における前記再生署名情報の前記不正署名情報群への追加は、可搬型である記憶媒体に追加記憶するようになすことを特徴とする3)又は4)項記載のコンテンツ情報認証再生装置。

【0021】

【発明の実施の形態】以下、本発明のコンテンツ情報の認証再生方法、及びコンテンツ情報認証再生装置の実施の形態につき、好適な実施例により説明する。図1は、

そのコンテンツ情報の認証再生方法を搭載するコンテンツ情報認証再生装置を含むコンテンツ情報認証記録再生システムの概略ブロック図であり、その構成と動作について概説する。

【0022】同図に示すコンテンツ情報認証記録再生システムは、デジタルコンテンツ部11、署名作成部14、及び信号記録部15よりなるコンテンツ情報認証記録装置10と、デジタルコンテンツ記録媒体20と、表示部61と、そしてコンテンツ情報認証再生装置40とより構成される。

【0023】そして、そのコンテンツ情報認証再生装置40は、記録信号読出し部41、デジタルコンテンツメモリ42、デコーダ44、署名検査部46、署名情報比較部47、署名情報記録部51、及び履歴管理部52より構成される。

【0024】次に、そのように構成されるコンテンツ情報認証記録再生システムの動作について概説する。まず、例えばMPEG (moving picture experts group)により策定された符号化方式により圧縮符号化されたビットストリームなどのデジタルコンテンツ部11に蓄積されるデジタルコンテンツは、署名作成部14により暗号化されて生成された署名情報と共に信号記録部15に供給され、そこでデジタルビデオテープなどのデジタルコンテンツ記録媒体20にそれらの供給された信号の記録がなされる。

【0025】このようにして記録されたデジタルコンテンツ記録媒体20は、正規の著作権の保護されるデジタルコンテンツが、著作権者に係る署名情報と共に記録されたものであるが、そのデジタルコンテンツ記録媒体20が不法コピーされて記録されたデジタルコンテンツ記録媒体20の署名情報は、署名作成部14により暗号化されて生成された署名情報とは異なる不正な署名情報として記録されるようになされる。

【0026】このようにして記録されたデジタルコンテンツ記録媒体20は、コンテンツ情報認証再生装置40によりデジタルコンテンツ及び署名情報の再生、とその復号がなされるが、次にそのコンテンツ情報認証再生装置40の動作について述べる。

【0027】まず、デジタルコンテンツ記録媒体20は記録信号読出し部41により再生され、再生されて得られるデジタルコンテンツはデジタルコンテンツメモリ42に、また署名情報は署名検査部46及び署名情報比較部47に供給される。

【0028】その署名情報比較部47では、予め署名情報記録部51に記録されている不正な署名情報テーブルと供給された署名情報とが比較され、不正な署名情報と一致する署名情報が検出されたとき、その検出結果に係る再生不可情報はデコーダ44に供給され、そのデコーダ44ではデジタルコンテンツメモリ42に一時記憶されたデジタルコンテンツの復号動作が中止される。

【0029】一方、署名情報比較部47に供給された署名情報と、予め署名情報記録部51に記録されている不正な署名情報テーブルとで一致する署名情報の検出がなされないときは、その署名情報比較部47では署名検査部46に対して署名検証実行指示信号が供給され、その署名検査部46では供給された署名情報の正当性について後述の暗号解析手法により署名情報の検証が行われる。

【0030】そして、署名情報が正当であると検証されたときは、デコーダ44に対して再生許可を与えるための再生可否情報が供給され、デコーダ44ではデジタルコンテンツメモリ42に一時記憶されるコンテンツ情報は、例えばMPEG標準により圧縮符号化のなされているデジタルコンテンツはそこでMPEG標準に基づいて復号化がなされ、復号化されて得られる映像信号は表示部61に供給されて、そのコンテンツの内容が表示される。

【0031】このようにして正当であるとして検証されたコンテンツの内容は表示されるが、反対に署名検証部46で署名情報が不正であるとして判定されたときは、デジタルコンテンツの復号を中止するための再生可否情報がデコーダ44に供給されて復号動作が中止されると共に、その判定された署名判定情報は署名情報比較部47に供給され、その署名情報比較部47では不正として判定された署名情報を署名情報記録部51に供給し、その署名情報記録部51では供給された署名情報は不正な署名情報テーブルに追加記録される。

【0032】そして、その署名情報記録部51に接続される履歴管理部52では、署名情報記録部51の不正な署名情報テーブルに追加記録される署名情報の記録日時、ないしは記録順に係る情報が記録履歴情報として記憶されるが、そのときに署名情報記録部51での記録量が所定の記録容量に近くなり、記録空き容量が所定値よりも少なくなったときは、例えば古い署名情報より順に消去がなされるようにされて記録領域が確保される。

【0033】このようにして、記録される署名情報テーブルが用いられることにより、署名検証部46でなされる署名検証のための処理時間が短縮されると共に、不正な署名情報テーブルに記録される不正なデジタルコンテンツの再生は、直ちにデジタルコンテンツ記録媒体20の再生、及びその表示が中止されるようになされる。

【0034】このようにして、コンテンツ情報認証再生装置40では、デジタルコンテンツ記録媒体20に記録されるデジタルコンテンツ、及び過去に再生されて記憶されている不正な署名情報を基にして、コンテンツ内容の再生可否に係る制御を短時間で行うと共に、不正な署名が検出されたときは不正な署名情報テーブルにその署名情報を追加するようにして、更に不正な署名情報に係る制御時間の短縮を図るものである。

【0035】以上、コンテンツ情報認証再生装置40の構成と動作について概説したが、更にその構成及び動作について述べる。図2に、実施例1によるコンテンツ情報認証記録再生システムの構成を示し、その動作について述べる。そして、その図2に示すシステムは前述の図1に示したシステムに機能を追加したものであり、次にその追加された機能を主に詳述する。

【0036】同図に示すコンテンツ情報認証記録再生システムはコンテンツ情報認証記録装置10a、デジタルコンテンツ記録媒体20、表示部61、そしてコンテンツ情報認証再生装置40aよりなっており、情報認証記録装置10aは前述の情報認証記録装置10に比してコピー制御フラッグ設定部12及びハッシュ関数演算部13が多く含まれて構成され、またコンテンツ情報認証再生装置40aは前述のコンテンツ情報認証再生装置40に比してハッシュ関数部43、制御部45、及び外部出力制御部48が多く含まれて構成されている。

【0037】次に、そのように構成されるコンテンツ情報認証記録装置10a、デジタルコンテンツ記録媒体20、及びコンテンツ情報認証再生装置40aの機能及び動作について更に述べる。

【0038】まず、デジタルコンテンツ部11に蓄積されているデジタルコンテンツはMPEGなどにより圧縮符号化された映像信号の他にも、MPEG以外の方式により符号化された画像信号、符号化音声信号、及びコンピュータプログラムなどの、いわゆるデジタル化された情報信号が用いられる。

【0039】そのようなデジタル化された情報信号は信号記録部15に供給されてデジタルコンテンツ記録媒体20に記録されるが、そのデジタルコンテンツ記録媒体20はデジタルVTR用の磁気テープの他に、デジタルデータを記録するストリーマ用などの磁気テープ、光磁気ディスク、DVDなどの光ディスク、更には半導体メモリなどのデジタル信号を記録できる記録媒体が用いられる。

【0040】そのようなデジタルコンテンツ記録媒体20に記録されるデジタルコンテンツは、コンテンツ情報認証再生装置40aにより再生が目的とされて使用されるが、そのコンテンツが他の記録装置に供給されてコピーされるなどの再利用に関しても管理される。

【0041】そのデジタルコンテンツの再利用に係る制御は、コピー制御フラッグ設定部12により設定されるコピー制御フラッグにより管理される様になされており、そのコピー制御フラッグは信号記録部15に供給されて、デジタルコンテンツ記録媒体20に記録される。

【0042】そのデジタルコンテンツ記録媒体20に記録されるコピー制御フラッグは、記録媒体20に記録されたデジタルコンテンツの他の記録媒体へのデジタルコピーを許可するか否かを示すフラッグであり、そ



のフラッグにより例えばCGMS (Copy Generation Management System) の手法が用いられてコピーの世代が1である「子」まで許すか、ないしは2である「孫」まで許すかなどの許可情報が、コピー制御フラッグ設定部12により設定される。

【0043】 そのようにして設定されてデジタルコンテンツ記録媒体に記録される情報として署名情報と署名設定フラッグ情報があるが、次にその署名情報及び署名設定フラッグ情報の生成について述べる。

【0044】 その署名情報は、デジタルコンテンツ記録媒体20に記録されるコンテンツの正当性を示すものであり、デジタルコンテンツ部11に記憶される情報の一部がハッシュ関数演算部13に供給され、そのハッシュ関数演算部13ではハッシュ関数などの一方向性関数が用いられて演算されてメッセージダイジェスト（以下MDとする）が得られ、その得られたMDは署名作成部14に供給される。

【0045】 その署名作成部14では、供給されたMDはコンテンツの著作権者により管理される秘密鍵データが用いられ、例えばRSA (Rivest Shamir Adelman) の3教授により開発された公開鍵暗号方式) 署名方式、ないしはDSS (Digital Signature Standard) 署名方式により作成される。

【0046】 そしてその署名作成部14では、署名情報と共に、その署名情報が記録されているか否かを示す署名情報フラッグ、例えば1ビットのバイナリデータで“0”は署名情報無し、“1”は署名情報ありを示す情報が作成され、それらの作成された署名情報及び署名情報フラッグは信号記録部15に供給される。

【0047】 以上のようにして、信号記録部15にはデジタルコンテンツ、コピー制御フラッグ、署名情報、及び署名情報フラッグなどの信号が供給され、それらの供給された信号はデジタルコンテンツ記録媒体20に記録される。

【0048】 そのようにしてコンテンツ情報認証記録装置10aにより記録されたデジタルコンテンツ記録媒体20はコンテンツ情報認証再生装置40aにより再生、及び復号化がなされるが、次にそのコンテンツ情報認証再生装置40aによる再生動作について述べる。

【0049】 まず、デジタルコンテンツ記録媒体20に記録されたデジタル信号は記録信号読み出し部41により読み出され、読み出された信号のうちデジタルコンテンツに係る信号はデジタルコンテンツ部42に、署名情報及び署名情報フラッグの両者は署名検証部46及び署名情報比較部47の両方に、またコピー制御フラッグ情報は外部制御出力部48にそれぞれ供給される。

【0050】 そして、それらの供給される情報の内の署名情報フラッグが“0”である場合は、デジタルコンテンツ記録媒体20には署名情報が記録されていないこ

とが示されているので、署名検証部46では署名情報の検証が行われる必要はなく、署名検証部46ではデコーダ44に再生が許可されるための再生可否情報が供給される。

【0051】 一方、署名情報フラッグが“1”であるときは、署名情報が記述されていることが示されており、その署名情報フラッグの供給された署名情報比較部47では、前述の図1を基に述べたと同様の方法により、供給される署名情報は予め署名情報記録部51に記録されている不正な署名情報テーブルと比較され、一致する署名情報が検出されたときは再生不可とされる情報が制御部45に供給される。

【0052】 また、一致する署名情報が検出されないときは、署名検証部46に署名検証実行指示情報が供給される。そして、その指示情報の供給された署名検証部46では、デジタルコンテンツ部42に一時記憶されたデジタルコンテンツの、所定のコンテンツ情報部分がハッシュ関数処理部によりハッシュ関数処理がなされてMD (Message Digest) 信号として供給され、その供給されたMD信号と検証の対象となる署名情報とは署名検証部46で著作権者により管理される公開鍵が用いられて検証動作がなされる。

【0053】 その検証動作の結果、署名情報が正当であるとして検証されたときは、デジタルコンテンツ部42に供給されたデジタルコンテンツ情報はデコーダ44に供給されて復号され、復号のなされた情報信号は表示部61に供給されて表示されるなどの、通常の再生動作がなされる。

【0054】 反対に、検証動作の結果署名情報が不正であるとして検証されたときには、デジタルコンテンツ記録媒体は不正であるとして、署名検証部46より制御部45に再生不可とされる再生可否情報が制御部45を介してデコーダ44に供給され、デコーダ44ではデジタルコンテンツの復号動作が中止されると共に、その不正として検証された署名情報は署名情報記録部51に供給され、そこに記録されている不正な署名情報テーブルに追加記録される。

【0055】 そして、その署名情報記録部51に追加記録される不正署名情報の書き込みは履歴管理部52により管理がなされ、不正署名情報記録可能な領域が所定量以上であるときはそこに不正署名情報が記録され、記録領域が所定量以下であるときは、例えば最も古い不正認証情報が消去され、新しく供給される不正認証情報が記録されるようになされる。

【0056】 さらに、このような不正署名情報が検出されたときは、表示部61に「デジタルコンテンツ記録媒体20は不正な記録媒体である」ことを表示し、ユーザにその検証の状況を知らせるようにする。

【0057】 このようにして、デジタルコンテンツ記録媒体20に記録されたデジタルコンテンツは、署名

情報、署名情報フラッグの検証が行われることにより、署名情報が記録されていないとき、及び署名情報の検証が正常になされたときにのみコンテンツ情報認証再生装置40aより復号された信号が表示部61に供給されて表示されるようになされている。

【0058】そして、また、そのコンテンツ情報認証再生装置40aには、記録信号読み出し部41により読み出されたデジタルコンテンツ記録媒体20の信号は外部出力制御部48を介して他の記録装置に供給され、コピー記録がなされるような機能が有されている。

【0059】その外部出力制御部48では、デジタルコンテンツ記録媒体20より読み出されたコピー制御フラッグ信号が供給されており、そのコピー制御フラッグ信号の内容、及び前記署名情報の検証結果に応じて他の記録装置に供給される信号の供給又は非供給の制御がなされる。

【0060】即ち、デジタルコンテンツ記録媒体20に記録されるデジタルコンテンツ、コピー制御フラッグ、及び署名情報が他の記録装置に供給されてデジタルコピーがなされるのは、そのコピー制御フラッグにコピー許可に係る情報があるときのみであり、そのときにデジタルコンテンツ信号及び付随される情報が他の記録装置に供給されるようになされている。

【0061】そして、前記のような不正署名情報が検出されたときには、記録信号読み出し部41より外部出力制御部48にコピー許可に係るコピー制御フラッグが、例えばコンテンツがデジタルコピー可能、又は1回だけコピー可能とされている場合であっても、デジタルコンテンツ等に係る情報が外部記録装置に供給されないように、記録信号読み出し部41より供給されるコピー制御フラッグはコピー禁止に係るフラッグに変更される。

【0062】次に、そのようにしてなされるコピー制御について述べる。図3に、コピー制御に係る信号記録の処理をフローチャートにより示し、説明する。

【0063】まず、ステップ1(S1)により、コピー制御フラッグ設定部12でコピー制御フラッグの設定がなされているか否かがチェックされ、設定されていないときはステップ3(S3)の署名の設定ステップに、またS1においてコピー制御フラッグ設定がなされているときはステップ2(S2)によりコピー制御フラッグの設定を行った後にS3の署名設定のステップに移る。

【0064】そのS3では、署名作成部14において署名の設定が行われた後にコンテンツ、署名情報、署名情報フラッグ、及びコピー制御フラッグの記録のステップ4に移行し、そのステップ4では信号記録部15によりそれらの信号のデジタルコンテンツ記録媒体20への記録動作がなされる。

【0065】次に、その記録されたデジタル記録コンテンツ読み出しの動作について述べる。図4に、そのデジタル記録コンテンツ記録媒体の読み出し制御に係る

信号再生の処理をフローチャートにより示し、説明する。

【0066】まず、ステップ11において記録されるコピー制御フラッグの検出が行われ、ステップ12においてそのコピー制御フラッグによりコピーが許可されているか否かがチェックされ、コピー可能とされるときはステップ13によりそのフラッグの内容が更新されて、外部出力制御部48より外部記録装置への信号記録のための信号供給が行われ、次のステップ15に移行する。

10 【0067】そして、S12における判定結果がコピー不可とされるときは、ステップ14により外部記録装置への出力が禁止され、署名情報フラッグの検出ステップ15に移行し、記録媒体20に記録される署名情報フラッグの検出が行われる。

【0068】そして、ステップ16においてその検出された署名情報フラッグが“1”であるか否かがチェックされ、“1”でないときは記録コンテンツ記録媒体の読み出し制御に係る処理が終了されてデジタルコンテンツ記録媒体20の再生動作が開始されると共に、検出された署名情報フラッグが“1”であるときはステップ17による署名情報の読み出しがなされる。

【0069】そのステップ17で読み出された署名情報はステップ18で、既に記憶されている不正署名テーブルに無いかどうかと比較され、不正署名情報があるとき(N o のとき)はステップ22に移りコンテンツの再生が停止され、一致する不正署名情報が無いとき(Y e s のとき)はステップ19の署名情報の検証動作がなされる。

【0070】そのステップ19でなされた検証結果を基に、ステップ20の署名検証によりコンテンツが正当か否かが判定され、正当であるときはコンテンツ記録媒体の読み出し制御に係る処理が終了されてデジタルコンテンツ記録媒体20の再生動作が開始されると共に、正当でないと判定されるときはステップ21により不正署名情報が署名情報記録部51に供給されて不正署名メモリテーブルに追加記録され、ステップ22でデジタルコンテンツ記憶媒体の再生が停止される。

【0071】以上のようにして、デジタルコンテンツ記録媒体20に記録されたコピー制御フラッグ、署名情報、及び署名情報フラッグ情報を基にして、記録されるコンテンツの再生、復号動作、及びそのコンテンツの外部接続機器へのコピーのための制御動作が行われる。

40 【0072】そして、その不正な署名情報は、予め署名情報記録部に記録される不正署名情報リストとの比較を行うことにより、不正な署名情報は演算が複雑である署名情報検証の作業を行わずに容易に得ることができるものである。

【0073】そこで、署名情報記録部51及び履歴管理部52に記録される不正署名テーブルに係る情報は取り外し可能な例えばフロッピディスク、ないしはICメモ

り素子などの記憶媒体に記録され、このコンテンツ情報認証再生装置40aとは異なるコンテンツ情報認証再生装置の署名情報記録部に、その記憶媒体に記憶された内容を記憶媒体と共に移動してコピーすることにより、その異なるコンテンツ情報認証再生装置は不正署名テーブルに記憶される署名情報を基に容易に不正署名の検出動作が行なわれる。

【0074】そして、このような不正署名の検出動作は、署名情報フラッグに「署名情報があり」とされる署名情報フラッグとして読み出されるときに行われる。そこで、仮に署名情報フラッグに記録される「署名情報があり」の情報が、「署名情報が無し」として改竄されて供給されるときには不正署名の検出動作は行われないことになる。

【0075】従って、署名情報フラッグのデジタルコンテンツ記録媒体への記録はただ単にコンテンツ情報のヘッダ領域に記録するなどのような簡単な記録方法ではなく、コンテンツ情報の中にその署名フラッグ情報を埋め込むようにして記録する必要がある。

【0076】即ち、その記録された署名情報の有り無しに係る署名情報フラッグ情報は、例えばコンテンツの中にウォーターマーク情報としてを埋め込むようにして行い、その記録された署名情報フラッグが署名情報有りから署名情報無しに変更されるような場合は、コンテンツの内容自体に破綻が生じ、そのコンテンツが正常に復号されて、表示されることがないようにする方法などが有る。

【0077】そのようなコンテンツの保護を行なうために、コンテンツ情報認証記録装置はコンテンツの少なくともその一部を暗号化して記録するようにし、コンテンツ情報認証再生装置ではその暗号化されたコンテンツを復号化して再生するようにする方法により実現することができる。

【0078】即ち、そのような暗号化されたコンテンツに署名情報有り無しに係る署名情報フラッグを埋め込み、その情報フラッグが改竄されたときに暗号化信号の解読がなされないように構成するのは比較的容易である。

【0079】以上、第1の実施例におけるコンテンツ情報認証記録装置によりデジタルコンテンツ記録媒体に記録したデジタルコンテンツの認証、及びコンテンツ情報の復号動作について述べたが、そのデジタルコンテンツは記録媒体に記録されて搬送される外に、通信路、ないしは放送伝送路が用いられて直接伝送されるようなデジタルコンテンツ情報に関しても同様なコンテンツ情報認証伝送受信システムを構成することができる。

【0080】図5に、コンテンツ情報認証伝送再生システムの構成を示す。同図に示す第2の実施例によるコンテンツ情報認証伝送装置10bは、前述のコンテンツ情

報認証記録装置10aに比して信号記録部15が伝送装置16に、またデジタルコンテンツ記録媒体20は伝送路30になっている点で異なっている。

【0081】そして、コンテンツ情報認証再生装置40bはコンテンツ情報認証再生装置40aに対して記録信号読み出し部41が受信装置49とされて構成されるがその他の構成は同一であり、従ってコンテンツ情報認証伝送再生システムは記録媒体の代りにデジタル伝送媒体を用いてデジタルコンテンツの配信を行う点で異なっており、その他の動作は前述の第1の実施例におけるコンテンツ情報認証記録装置と同様である。

【0082】このようにして、第1の実施例で示したコンテンツ情報認証記録再生システムにおけるデジタルコンテンツの認証、及びコンテンツ情報の復号動作については第2の実施例で示すコンテンツ情報認証伝送再生システムにおいても同様に行われる。

【0083】そして、第2の実施例ではデジタルコンテンツ記録媒体20の代りに伝送路30が用いられているが、その伝送路は署名情報記録部に記録された不正署名情報テーブルの伝送に使用することもできる。

【0084】図6に、その不正署名情報テーブルを記憶する記憶媒体をネットワークサーバ50に設け、不正署名情報は伝送ネットワークを介して伝送する、ないしはネットワークを介して取得する場合のコンテンツ情報認証再生装置40cの構成を示し説明する。

【0085】同図に示すコンテンツ情報認証再生装置40cは、前述の図5におけるコンテンツ情報認証再生装置40bの構成に比して署名情報記録部51及び履歴管理部52はなく、署名検証部46はネットワークインタフェース31及び32を介して、ネットワークサーバ50の中にある署名情報記録部51及び履歴管理部52が接続されている。

【0086】そのように接続される署名検証部における不正署名情報の検証は、前述の図2に示した署名検証部46と同様に行われ、検証作業により不正なコンテンツ及び媒体であると認められた場合には、その作業の行われたコンテンツ情報認証再生装置における再生可否情報は再生不許可もしくは再生停止の指示信号を制御部45に供給されると共に、その検証された不正署名情報はネットワークインタフェース31、及び32を介してネットワークサーバ50の署名情報記録部51に供給される。

【0087】そして、その不正署名情報は、ネットワークサーバ50にネットワーク接続される複数のコンテンツ情報認証再生装置により共有されるようになされ、その不正署名情報リストは複数のコンテンツ情報認証再生装置により共用して利用されると共に、それぞれのコンテンツ情報認証再生装置により検証された不正署名情報のそれぞれはそのネットワークサーバ50に供給される。

【0088】そのネットワークサーバ50には複数のコンテンツ情報認証再生装置により検出された多くの不正署名情報が供給されて、短期間に不正署名情報に係るデータベースが構築されることとなり、各々のコンテンツ情報認証再生装置による検証作業が減少される。

【0089】そして、そのデータベースを記憶するネットワークサーバの署名情報記録部の容量は大きく設定されるが、その署名情報記録部に供給される不正署名情報は履歴管理部52によりなされており、署名情報記録部51における不正署名情報記録領域に記録可能とされる空き領域があるときは、その不正署名情報は署名情報記録部に記録され、記録可能な領域が不足している場合には、例えば最も古い不正認証情報が消去され、新しく供給された不正認証情報が記録されるようになされる。

【0090】そのようにして記録される不正認証情報は、前述の第1の実施例におけるコンテンツ情報認証再生装置の場合では、不正署名情報リストをフロッピディスク、ないしはICメモリ素子を介して異なるコンテンツ情報認証再生装置の間でデータの共有を行なうようにしていたが、ネットワーク結合による不正署名データの共有は、新たに検証された不正署名データに対するデータの更新が実時間で、且つ記憶媒体の交換作業を伴わなく容易になされるため、それぞれのコンテンツ情報認証再生装置における署名データ検証のための作業を削減することができるものである。

【0091】以上、ネットワークサーバ50に署名情報記録部51を有し、不正署名データを共有する第3の実施例について述べたが、次にそのネットワークサーバに署名検証部を設ける場合の例について述べる。

【0092】図7は、そのネットワークサーバに署名検証部を設ける場合の第4の実施例によるコンテンツ情報認証再生装置の構成を示したものであり、それらの動作について説明する。

【0093】即ち、同図に示すコンテンツ情報認証再生装置40dは、前述の図6に示した第3の実施例によるコンテンツ情報認証再生装置40cに比し、署名検証に係るハッシュ関数部43、署名検証部46、及び署名情報比較部47の回路部がないが、それらはネットワークインタフェース31a及びネットワークインタフェース31bを介してネットワークサーバ50aの中にあるハッシュ関数部43、署名検証部46、及び署名情報比較部47に接続されるようになされて構成されている点で異なっている。

【0094】このように構成されるコンテンツ情報認証再生装置40dの動作は、コンテンツ情報認証再生装置40cの動作に比し、署名の検証に係る動作が必要ときはネットワークを介してネットワークサーバ50aに検証作業を要求し、そのサーバ部50aでは検証作業により得られた結果に応じ、コンテンツ情報認証再生装置40dに関する再生可否情報はネットワークを介して

制御部45に供給されると共に、不正な署名情報に関しては前述と同様にして署名情報記録部51にその不正署名情報の記録が行なわれようになされる。

【0095】即ち、コンテンツ情報認証再生装置40dよりネットワークサーバ50aに署名情報、署名情報フラッグ、及びデジタルコンテンツのメッセージダイジェストを作成するために必要なコンテンツの一部の情報は、ネットワークインタフェース31aを介してネットワークサーバ50aに供給され、そのネットワークサーバ側ではネットワークインタフェース32aを介して供給されるそれらの情報信号を得て署名の認証作業が行なわれるようにする。

【0096】このようにして、ネットワークを介して行う署名認証作業用の信号、及び再生可否情報などは、ネットワークに接続される他のコンピュータにより改竄される可能性が有るので、ネットワークを介して伝送される信号は十分に強度の高い暗号化がなされていることが望ましい。

【0097】そして、ネットワークサーバ50aでは、署名情報記録部に記録される不正署名データが外部からのアクセスにより消去される、あるいは正当な署名情報が不正署名情報として記録されるなどのような改竄がなされることを防止するためにも十分に保護される暗号化システムにより構成することが望ましいが、その他に記録された不正署名データの再検証を定期的に行うなどによる記憶データの維持管理が必要である。

【0098】以上、第1～第4の実施例により、記憶される不正署名データを用いて高速且つ容易に署名情報の検証を行う記録再生方法、伝送受信方法、及びそれらを搭載する装置の構成、及びそれらの動作について述べた。

【0099】それらの記録及び伝送装置により署名情報、及び署名フラッグ情報が付されたデジタルコンテンツ情報の再生、ないしは受信に際し、そのデジタルコンテンツと記録媒体、ないしは伝送媒体で伝送される署名情報の認証を行い、不正なコンテンツ及び媒体であると検証されたときには、その再生を中止すると共に、再度その不正署名情報を有する媒体が再生されようとなるときは、前記認証の処理を行うことなくコンテンツの再生を不許可もしくは停止させることができ、処理時間の短縮、及び処理の簡易化ができる。

【0100】そして、その不正署名情報は、特に取り外し可能な記録媒体ないしはメモリ素子にその不正署名情報を記録するようにしたので、それらの不正署名情報記録媒体ないしはメモリ素子を複製し、複数の再生装置ないしは受信装置にそれらの不正署名情報記録媒体を供給することにより複数の装置で署名認証のための作業の高速化、および簡易化がなされる。

【0101】また、複数の再生装置ないしは受信装置をネットワークにより結合し、ネットワークを介して不正

署名情報の供給を行う場合には、複数の装置のうちの1つの装置により検証された不正署名情報を同時に共有することができるため、更に簡便に署名情報が検証されて動作する再生装置ないしは受信装置を構成することができる。

【0102】さらに、ネットワーク上に接続されているネットワークサーバに不正署名情報を検証して得、その得られた不正署名情報を記録するようにしたので、ネットワークに接続される全ての再生装置ないしは受信装置は、署名情報の検証機能を有していない場合であっても高演算機能を備えたネットワークサーバにより検証された署名情報を基にデジタルコンテンツの再生、ないしは受信を行なうことができる認証処理速度が早く、且つ低価格であるコンテンツ情報認証再生装置を構成することができるものである。

【0103】

【発明の効果】請求項1記載の発明によれば、正当な権利の基に制作されたデジタルコンテンツに、そのデジタルコンテンツの制作に係る署名情報が付加されて記録されたデジタルコンテンツ記録媒体を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたデジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはデジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【0104】また、請求項2記載の発明によれば、正当な権利の基に制作されたデジタルコンテンツに、そのデジタルコンテンツの制作に係る署名情報が付加されて伝送されたデジタルコンテンツ情報を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたデジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはデジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報認証再生方法を提供できる効果がある。

【0105】また、請求項3記載の発明によれば、正当な権利の基に制作されたデジタルコンテンツに、そのデジタルコンテンツの制作に係る署名情報が付加されて記録されたデジタルコンテンツ記録媒体を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたデジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはデジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理手段を簡易に構成できると共に認証処理時間を削減したコンテンツ情報認証再生装置の構成を提供できる効果がある。

【0106】また、請求項4記載の発明によれば、正当な権利の基に制作されたデジタルコンテンツに、そのデジタルコンテンツの制作に係る署名情報が付加されて伝送されたデジタルコンテンツ情報を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたデジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはデジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理手段を簡易に構成できると共に認証処理時間を削減したコンテンツ情報認証再生装置の構成を提供できる効果がある。

【0107】また、請求項5記載の発明によれば、請求項3及び4記載の効果に加え、特に署名比較は、取り外し可能な可搬型記憶媒体に記憶された不正署名情報テーブルを用いて行うようにしているため、更に認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【0108】また、請求項6記載の発明によれば、請求項3及び4記載の効果に加え、特に署名比較は、ネットワークに接続されるネットワークサーバの記憶媒体をアクセスし、その記憶媒体に記憶される不正署名情報テーブルのデータを用いて行うようにしているため、認証処理に係る処理工程を更に簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【0109】また、請求項7記載の発明によれば、請求

項 3 及び 4 記載の効果に加え、特に署名検証は、ネットワークに接続され再生署名情報の正当性の検証機能を有するネットワークサーバに、再生署名情報を伝送し、そのネットワークサーバより再生署名情報の正当性の検証結果に係る署名検証情報はネットワークを介して得られるようにしているため、さらに認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【0110】また、請求項 8 記載の発明によれば、請求項 3 及び 4 記載の効果に加え、特にデジタルコンテンツ再生の中止に係る動作は、圧縮符号化されたデジタルコンテンツ情報の復号を行う復号器に、再生が不許可であることを示す再生不可情報を供給するようにしているため、認証処理に係る処理工程に係る遅延時間のために誤って復号化されたデジタルコンテンツ情報が再生されてしまうといったような誤動作を防止したコンテンツ情報の認証再生方法を提供できる効果がある。

【0111】また、請求項 9 記載の発明によれば、請求項 3 及び 4 記載の効果に加え、特に記録媒体の再生の中止に係る動作は、デジタルコンテンツ記録媒体に、その記録されるデジタルコンテンツが他の記録媒体にコピーすることを許可するコピー許可情報が記録されている場合であっても、そのコピーのための信号供給を中止する動作を同時に行うことによりコピー許可に係る誤動作を防いだコンテンツ情報の認証再生方法を提供できる効果がある。

【0112】また、請求項 10 記載の発明によれば、請求項 3 及び 4 記載の効果に加え、特に再生署名情報の不正署名情報テーブルへの追加は、可搬型の記憶媒体に追加記憶するようにしているため、その記憶された不正署名情報テーブルは他のコンテンツ情報の認証再生方法に用いることができるため、その認証方法を搭載するコンテンツ情報の認証再生装置に係る認証処理の処理工程を簡易にできると共に、認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

#### 【図面の簡単な説明】

【図 1】本発明のコンテンツ情報認証再生装置に係るコンテンツ情報認証記録再生システム構成の概略を示す図である。

【図 2】本発明の第 1 の実施例に係るコンテンツ情報認

証記録再生システムの構成を示す図である。

【図 3】本発明の実施例によるコンテンツ情報認証記録装置に係る記録信号の動作を示すフローチャートである。

【図 4】本発明の実施例によるコンテンツ情報認証再生装置に係る再生信号の動作を示すフローチャートである。

【図 5】本発明の第 2 の実施例に係るコンテンツ情報認証記録再生システムの構成を示す図である。

10 【図 6】本発明の第 3 の実施例に係るコンテンツ情報認証再生装置の構成を示す図である。

【図 7】本発明の第 4 の実施例に係るコンテンツ情報認証再生装置の構成を示す図である。

#### 【符号の説明】

10、10a コンテンツ情報認証記録装置

10b コンテンツ情報認証伝送装置

11 デジタルコンテンツ部

12 コピー制御フラグ設定部

13 ハッシュ関数演算部

20 14 署名作成部

16 伝送装置

20 デジタルコンテンツ記録媒体

30 伝送路

31、31a、32、32a ネットワークインタフェース

40、40a、40b、40c、40d コンテンツ情報認証再生装置

41 記録信号読出し部

42 デジタルコンテンツメモリ

30 43 ハッシュ関数部

44 デコーダ

45 制御部

46 署名検査部

47 署名情報比較部

48 外部出力制御部

49 受信装置

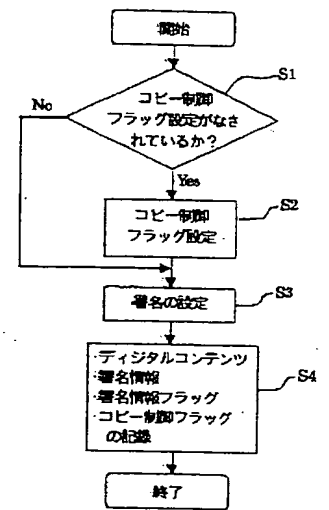
50、50a ネットワークサーバ

51 署名情報記録部

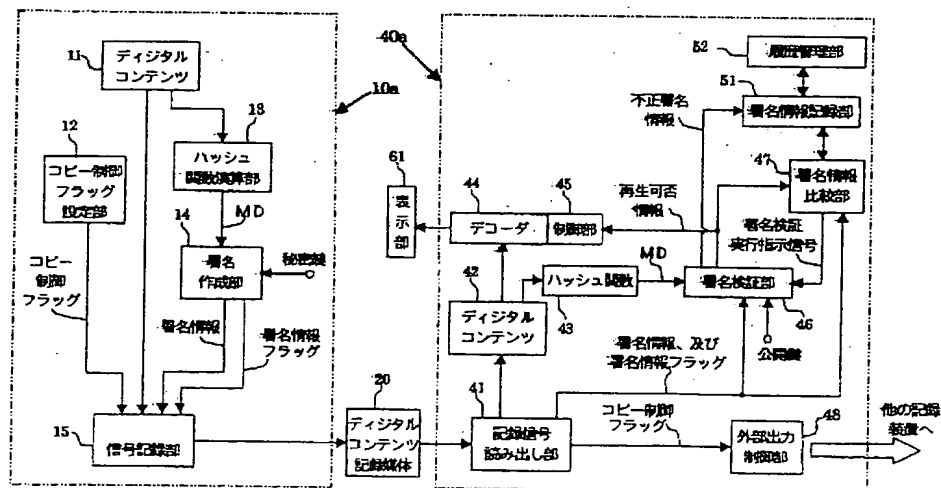
52 履歴管理部

40 61 表示部

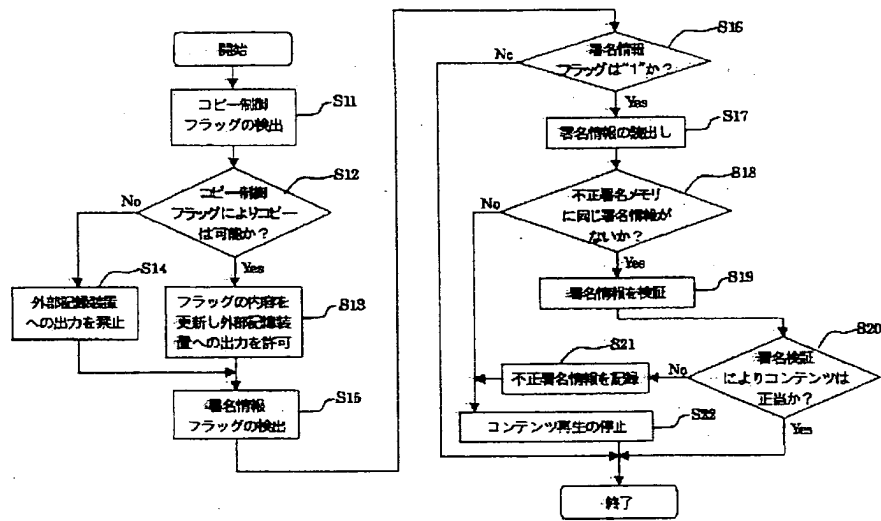
【圖 3】



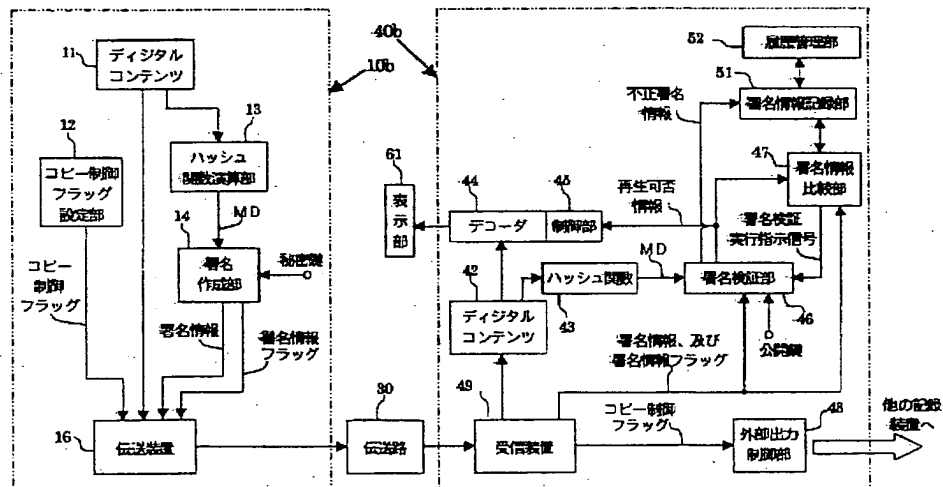
【图 2】



【図4】

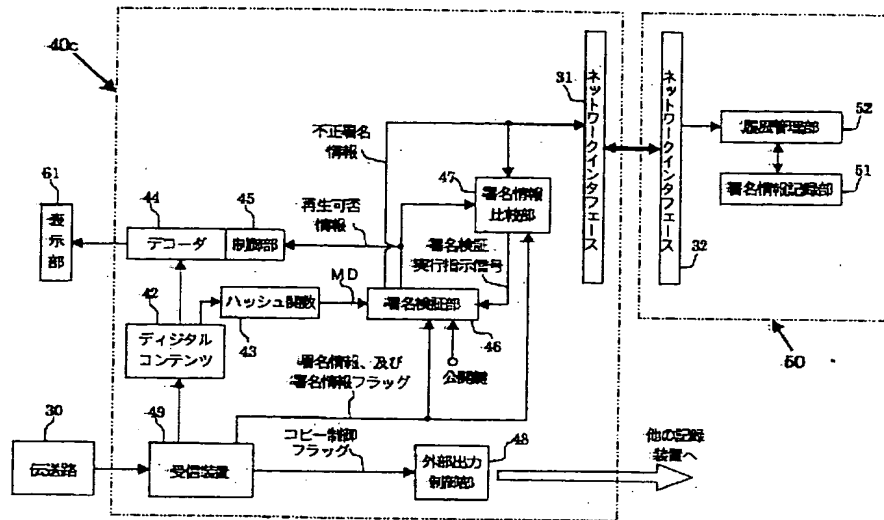


【図5】

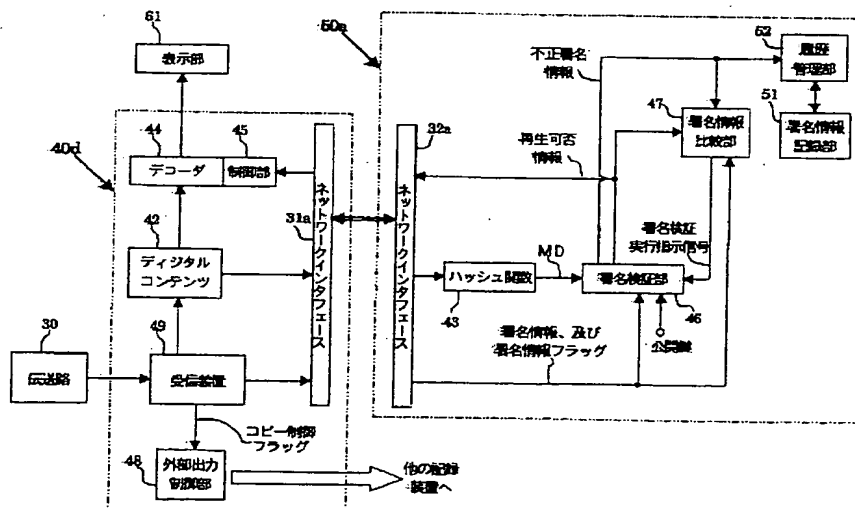




【図6】



【図7】



フロントページの続き

Fターム(参考) 5B017 AA07 CA16

5C053 FA13 FA22 FA25 GA11 GB37

HA40 JA21

5J104 AA07 AA09 KA01

**THIS PAGE BLANK (UCPTO)**